联 合 国 A/HRC/14/46

大 会

Distr.: General
5 May 2010
Chinese
Original: English

人权理事会
第十四届会议
议程项目 3
增进和保护所有人权——公民权利、政治权利、经济、社会和文化权利，包括发展权

反恐中注意增进和保护人权与基本自由问题特别报告员马丁·舍伊宁先生的报告*

确保情报机构在反恐中尊重人权的法律和体制框架及措施，包括对情报机构的监督——良好做法汇编**

摘要

本文件系根据人权理事会的要求，由反恐中注意增进和保护人权与基本自由问题特别报告员编写，介绍了确保情报机构在反恐中尊重人权的法律和体制框架以及采取的措施，包括对有关机构的监督，对这方面的良好做法进行了汇编。汇编是在征求各方面意见后取得的结果，其中各国政府、专家和实际工作者以不同方式提供了投入。报告特别吸收了各国政府在 2010 年 5 月 1 日截止日期之前提交的材料。这些材料将以本文件的增编形式转发(A/HRC/14/46/Add.1)。

这项工作的成果是，找出了 35 种良好做法。这些良好做法是从世界各地很多国家现有的和正在形成的做法中提炼出来的。汇编还借鉴了各项国际条约、国际组织的决议和区域法院的司法判例。

* 迟交。

** 由于报告篇幅大大超过大会有关决议现行规定的页数限制，因此报告附件和脚注不译，原文照发。

这些良好做法的实质内容，在评注中做了说明，一般是对 35 种做法中的每一种做单独介绍。良好做法的来源在评注的脚注中说明，包括提到具体国家。

“良好做法”的概念，是指有助于在情报部门的工作中促进人权和尊重法治的各种法律和体制框架。“良好做法”不仅仅指符合国际法，包括人权法所要求的做法，而且还包括这些具有法律约束力义务以外的内容。

汇编中所收入的 35 个方面的良好做法，可归为四个不同的大类，即法律依据(做法 1-5)，监督和问责(做法 6-10 和 14-18)，切实遵守人权(做法 11-13 和 19-20)和情报机构具体职能的有关问题(做法 21-35)。

目录

一. 导言*

1. 这份“关于情报部门的法律和体制框架及对情报部门进行监督的良好做法汇编”，是人权理事会授权开展的一项磋商进程的成果，理事会要求特别报告员：

> “……征求各国和其他主要利益攸关方的意见，编写一份关于确保情报机构在反恐中尊重人权，包括对情报机构监督的法律和体制框架及措施的良好做法汇编(人权理事会第 10/15 号决议第 12 段)。”

2. 情报部门[1] 在保护国家和人民免受包括恐怖主义在内的对国家安全的威胁方面，发挥着至关重要的作用。情报部门还可帮助国家履行其实在法义务，保障其管辖下的所有个人的人权。因此，有效履行职能和保护人权可以成为情报部门相得益彰的两个目标。

3. 这份汇编是从世界各地很多国家现有的和正在形成的做法中提炼出来的。这些做法主要源自各国的法律、体制模型、司法判例和国家监督机构及一些公民社会组织的建议。汇编还吸收了国际条约、国际组织的决议和区域法院的判例。在这方面，“良好做法”的概念系指有助于在情报部门的工作中促进人权和尊重法治的法律和体制框架。“良好做法”不仅仅指国际法，包括人权法所要求的做法，而且还包括这些具有法律约束力义务以外的内容。

4. 很少国家在他们对情报部门的法律和体制框架中和对情报部门的监督中包括了以下列出的所有做法。一些国家准备采纳这 35 种良好做法中的大多数做法。还有一些国家可能先作出承诺，采纳少数他们认为对促进情报部门及监督机构尊重人权最为重要的做法。

5. 本汇编的目的不是颁布一套任何时候在世界上的任何地方都能适用的规范性标准。因此，本报告中所介绍的良好做法，行文上采用了说明的方式，而没有使用法律的规范性语言。然而，仍有可能找出一些带有共性的、有助于情报部门尊重法治和人权的做法。

6. 人权理事会授权编写这份良好做法汇编的前提，是情报部门在反恐中的作用。然而，应当指出的是，对情报部门反恐活动适用的法律和体制框架，不可能

* The Special Rapporteur would like to acknowledge the contribution of Hans Born and Aidan Wills of the Geneva Centre for the Democratic Control of Armed Forces for conducting a background study and assisting in the preparation of this compilation. Furthermore, the Special Rapporteur is grateful to Governments, as well as members of intelligence oversight institutions, (former) intelligence officials, intelligence and human rights experts as well as members of civil society organizations for their participation in the consultation process which led to this compilation.

[1] For the purposes of the present study, the term ‘intelligence services’ refers to all state institutions that undertake intelligence activities pertaining to national security. Within this context, this compilation of good practice applies to all internal, external, and military intelligence services.

与对该部门适用的更一般的法律和体制框架分隔开来。尽管自 2001 年以来国际恐怖主义大大改变了情报机构行动的舞台，但这种改变的影响则超出了反恐领域。

7. 这份汇编重点列举了很多国家法律和体制模型的良好做法。然而必须指出，列举国家法律的具体规定或体制模型，并不意味着在总体上认可这些法律和体制就是在反恐中保护人权的良好做法。而且，特别报告员还愿强调，建立良好做法的法律和体制框架十分重要，但还不是确保情报部门在反恐活动中尊重人权的充分条件。

8. 下文介绍的 35 个方面的良好做法，可大体分为四组，即法律依据(1-5)，监督和问责(6-10、14-18)，实际遵守人权(11-13、19-20)和情报机构具体职能的有关问题(21-35)。为便于阐述，对做法的分组略高于小标题的数量。

二. 情报部门的法律和体制框架及对情报部门监督的良好做法汇编

A. 授权和法律依据

做法 1. 情报部门在保护国家安全和维护法治方面起着重要作用。情报部门的主要目标，是收集、分析和递交情报，帮助决策人和其他公共实体采取措施保护国家安全，包括保护人民和他们的人权。

9. 情报部门的职能各国之间有所不同，然而，收集、分析和递交有关保护国家安全的情报，是大多数情报部门的一项核心任务。[2] 实际上，很多国家将本国情报部门的作用限于这项任务。这是一种良好做法，因为它可以防止情报部门从事与安全有关的其他活动，而那些活动已经有其他公共机关负责，如果由情报部门来做，可能构成对人权的特殊威胁。除了对情报部门所开展的活动类型作出规定外，很多国家还将这些活动的依据限于保护国家安全。尽管对国家安全的理解各国有所不同，但这方面的良好做法是，由议会通过立法，明确规定国家安全及其内涵。[3] 必须确保情报部门的活动限于维护公开定义的国家安全所载的价值观。

[2] Germany, Federal Act on Protection of the Constitution, section 5(1); Croatia, Act on the Security Intelligence System, article 23 (2); Argentina, National Intelligence Law, article 2 (1); Brazil, Act 9,883, articles 1(2) and 2(1); Romania, Law on the Organisation and Operation of the Romanian Intelligence Service, article 2; South Africa, National Strategic Intelligence Act, section 2 (1).

[3] Australia, Security Intelligence Organisation Act, section 4.

在很多地区，维护国家安全必然包括保护人民和他们的人权，[4] 实际上，一些国家明确将保护人权列入国家情报部门的核心职能。[5]

做法 2. 通过法律对情报部门的授权作出严格和准确的规定，公开发表。授权应严格限于保护合法的国家安全利益，在公开发表的法律或国家安全政策中提出，并明确情报部门负责处理的对国家安全的威胁所在。如果在这些威胁中包括恐怖主义，必须以严格和准确的措辞作出规定。

10. 对情报部门的授权是一项重要手段，确保情报部门的活动(包括在反恐条件下)为国家和人民的利益服务，而不构成对宪法秩序和/或人权的威胁。在大多数国家，对情报部门的授权是由议会颁布、[6] 以法律明确界定，并公开发表的。这方面的良好做法是，对授权作出严格和准确的规定，一一列出情报部门负责应对的所有对国家安全的威胁。[7] 明确和准确的授权有利于问责制的实行，使监督和审查机关能够要求情报部门对履行具体职能承担责任。最后，明确定义各项威胁，在反恐条件下尤其重要；很多国家都已通过立法，对恐怖主义以及恐怖主义组织和活动做了准确的定义。[8]

做法 3. 国家法律对情报部门的权力和权限作出明确和全面的规定。要求情报部门使用这些权力只能用于相应的目的。具体而言，给于情报部门用于反恐目的的任何权力，只能用于既定目的。

[4] General Assembly resolutions 54/164 and 60/288; Council of the European Union, European Union Counter-Terrorism Strategy, doc. no 14469/4/05; para. 1; Inter-American Convention Against Terrorism, AG/RES. 1840 (XXXII-O/02), preamble; Council of Europe, Committee of Ministers, Guidelines on human rights in the fight against terrorism, article I.

[5] Croatia (footnote 2), article 1.1; Switzerland, Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure, article 1 ; Brazil (footnote 2), article 1(1).

[6] Norway, Act relating to the Norwegian Intelligence Service, section 8; Bosnia and Herzegovina, Law on the Intelligence and Security Agency, articles 5-6; Brazil (footnote 2), Article 4; Canada, Security Intelligence Service Act, sections 12-16; Australia (footnote 3), section 17. This practice was also recommended in Morocco, Instance equité et réconciliation, rapport final, Vol. I, Vérité, equité et réconciliation, 2005, chapitre IV, 8-3 (hereafter Morocco - ER Report); European Commission for Democracy Through Law, Internal Security Services in Europe, CDL-INF(1998)006, I, B (b) and (c) (hereafter Venice Commission (1998)).

[7] Canada (footnote 6), section 2; Malaysia, report of the Royal Commission to enhance the operation and management of the Royal Malaysia Police of 2005, (hereafter Malaysia – Royal Police Commission), 2.11.3 (p. 316); Croatia (footnote 2), article 23(1); Australia (footnote 3), section 4; Germany (footnote 2), sections 3(1) and 4; United States of America, Executive Order 12333, article 1.4 (b).

[8] Romania, Law on Preventing and Countering Terrorism, Article 4; Norway, Criminal Code, Section 147a; New Zealand, Intelligence and Security Service Act, Section 2.

11. 情报部门的一切权力和权限均由法律作出规定，[9] 这是法治的基本原则。一一列出情报部门的权力和权限，有助于提高透明度，使人民能够知道可能对他们使用哪些权力。由于情报部门所掌握的很多权力有可能侵犯人权和基本自由，因此这一点尤其重要。[10] 这方面的做法与前面一种做法(做法 2)密切相关，因为对情报部门的授权可用来确定他们须在什么框架下使用法律给予他们的权力。[11] 很多国家的法律明确禁止滥用权力，情报部门只能在十分具体的目的上使用他们的权力。这在反恐条件下尤其如此，因为很多情报部门为了反恐而享有更大的权力。

做法 4. 所有情报部门的组建都必须通过公开颁布的法律，并在法律下运作，必须符合宪法和国际人权法。情报部门只能按照国家法律的规定，依法开展活动或受命开展活动。使用非公开发表的子规定须受到严格限制，且这些规定必须得到公开颁布的法律授权或在其规定范围之内。非公开发表的规定不能作为任何限制人权活动的依据。

做法 5. 明确禁止情报部门采取任何违背宪法或国际人权法的行动。这方面的禁止不仅适用于情报部门在本国境内的行为，而且也适用于他们在国外的活动。

12. (4 和 5)情报部门是国家机关，因此与其他行政部门一样，受到国家和国际法相关规定的约束，特别是人权法。[12] 这意味着他们必须根据公开发表的符合国家宪法的法律，以及该国的国际人权义务运作。国家不能以本国法为理由违反国际人权法，也不能违反任何其他国际法律义务。[13] 法治要求情报部门的各项活动和政府行政部门给予他们的指示，一切工作都必须遵守上述法体。[14] 因

[9] Croatia (footnote 2), Articles 25-37; Lithuania, Law on State Security Department, Article 3; Germany (footnote 2), Section 8. See also: South African Ministerial Review Commission, p. 157; Canada, MacDonald Commission, p. 410; Morocco - IER report, 8-3; Malaysia, Royal Police Commission, 2.11.3 (p. 316).

[10] Council of Europe (footnote 4), article V (i); European Court of Human Rights, *Malone v. The United Kingdom*, para. 67.

[11] Canada, MacDonald Commission, pp. 432, 1067.

[12] General Assembly resolution 56/83, annex, article 4 (1); Dieter Fleck, “Individual and State responsibility for intelligence gathering”, *Michigan Journal of International Law* 28, (2007), pp. 692-698.

[13] General Assembly resolution 56/83, annex, article 3.

[14] Brazil (footnote 2), article 1(1); Sierra Leone, National Security and Central Intelligence Act, article 13(c); United States Senate, Intelligence activities and the rights of Americans¸ Book II, final report of the select committee to study governmental operations with respect to intelligence (hereafter: Church Committee), p. 297; Canada, MacDonald Commission, pp. 45, 408; ECOWAS Draft Code of Conduct for the Armed Forces and Security Services in West Africa (hereafter ECOWAS Code of Conduct), article 4; Committee of Intelligence and Security Services of Africa, memorandum of understanding on the establishment of the Committee of Intelligence and Security Services of Africa (hereafter CISSA MoU), article 6.

此，禁止情报部门采取或要求情报部门采取任何可能违反国家法律、宪法或国家人权义务的行动。在很多国家，这些要求是不言而喻的，然而，应当指出的良好做法是，国家立法明确提及这些宽泛的法律义务，特别是尊重人权的义务。[15] 有关情报部门内部程序和活动的次级规定有时不公开发表，以便保护他们的工作方法。这类规定不能作为侵犯人权活动的依据。良好做法是任何次级规定必须建立在适用的公开法律基础上并遵守有关法律。[16]

B. 监督机构

做法 6. 情报部门受到内部、行政、议会、司法和一些特别监督机构的共同监督，后者的授权和权力是根据公开颁布的法律。对情报部门的有效监督制度，应至少包括一个既独立于情报部门又独立于行政部门的文职机构。这些监督机构的综合职能涵盖了情报部门工作的所有方面，包括他们遵守法律的情况，情报活动的作用和效率，情报部门的资金来源和他们的行政事务。

13. 与情报部门一样，监督情报部门活动的机构也应依法设立，在有些情况下，依宪法设立。[17] 对情报部门的监督没有单一的模式，然而在全面的监督系统中通常包括以下内容：[18] 情报部门内部的管理和控制机制；[19] 行政部门的监

[15] Argentina (footnote 2), article 3; Bulgaria, Law on State Agency for National Security, article 3 (1) 1-2; Bosnia and Herzegovina (footnote 6), article 1; Brazil (footnote 2), article 1(1); Croatia (footnote 2), article 2(2); Ecuador, State and Public Safety Act, article 3; Lithuania (footnote 9), article 5; Romania, Law on the National Security of Romania, articles 5, 16; Mexico (reply).

[16] Argentina (footnote 2), article 24; Venice Commission (1998), I, B (b) and (c); Malaysia, Royal Police Commission 2.11.3 (p. 316); Kenya, National Security Intelligence Act, article 31; South Africa, Truth and Reconciliation Commission of South Africa, report, vol. 5, chap. 8, p. 328.

[17] Germany, Basic Law for the Federal Republic of Germany, article 45d; South Africa, Constitution, articles 209-210.

[18] See S/2008/39, para. 6. While not included in the present compilation, it should be underlined that civil society organizations also play an important role in the public oversight of intelligence services; see reply of Madagascar.

[19] For an elaboration on internal management and control mechanisms, see South African Ministerial Review Committee, p. 204; European Commission for Democracy through Law, report on the democratic oversight of the security services, CDL-AD(2007), point 131 (hereafter Venice Commission (2007)); OECD DAC handbook on security system reform: supporting security and justice; United Kingdom, Intelligence Security Committee, annual report 2001-2002, p. 46. See also The former Yugoslav Republic of Macedonia (reply).

督；[20] 议会机构的监督；[21] 以及专门和/或司法监督机构。[22] 这套多层次的监督制度的一个良好做法，是包括至少一个完全独立于情报部门和行政部门的机构。这种做法可以保证对情报部门监督的权力分开：授权、执行和接受情报活动成果的机构，不能都是负责监督情报活动的机构。情报部门工作的各个方面均须受到一个或多个外部机构的监督。监督制度的一个主要职能，是监察情报部门是否遵守了相应的法律，包括人权。监督机构有权要求情报部门和情报部门的雇员对任何违反法律的行为负责。[23] 此外，监督机构还评估情报部门的绩效。[24] 这包括研究情报部门是否有效、节约地使用了给他们的公共拨款。[25] 有效的监督制度在情报领域尤其重要，因为这些部门的大部分工作是秘密进行的，因此公众难以监督。情报监督机构有利于提高公众对情报部门工作的信任和信心，确保情报部门根据遵守法治和人权的要求履行他们的法定职能。[26]

做法 7. 监督机构有权并有资源和专门知识，能够自己启动和展开调查，并可完全不受限制地获得履行任务所必需的信息、接触有关官员和进入有关设

[20] On executive control of intelligence services, see Croatia (footnote 2), article 15; United Kingdom, Security Services Act, sections 2(1), 4(1); Argentina (footnote 2), article 14; Netherlands, Intelligence and Security Services Act, article 20(2); Sierra Leone (footnote 14), article 24; Bulgaria (footnote 15), article 131; Azerbaijan, Law on Intelligence and Counter-Intelligence Activities, article 22.2.

[21] For legislation on parliamentary oversight of intelligence services, see Albania, Law on National Intelligence Service, article 7; Brazil (footnote 2), article 6; Romania (footnote 2), article 1; Ecuador (footnote 14), article 24; Botswana, Intelligence and Security Act, section 38; Croatia (footnote2), article 104; Switzerland (footnote 5), article 25, Loi sur l'Assemblée fédérale, article 53(2); Germany (footnote 17), article 45d; Bulgaria (footnote 15), article 132; The former Yugoslav Republic of Macedonia (reply). See also Morocco, IER Report, p. 11. In Latvia, the National Security Committee of the parliament (*Saeima*) is responsible for parliamentary oversight of the intelligence service (reply); Georgia, Law on Intelligence Activity, article 16.

[22] For specialized intelligence oversight bodies, see Norway, Act on Monitoring of Intelligence, Surveillance and Security Services, article 1; Canada (footnote 6), sections 34-40; Netherlands (footnote 20), chapter 6; Belgium, Law on the Control of Police and Intelligence Services and the Centre for Threat Analysis, chapter 3.

[23] For mandates to oversee intelligence services' compliance with the law, see Lithuania, Law on Operational Activities, article 23(2)1-2; Croatia (footnote 2), article 112; Norway (footnote 22), section 2. In South Africa, the Inspector-General for intelligence examines intelligence services' compliance with the law and Constitution; see South Africa, Intelligence Services Oversight Act, section 7(7) a-b.

[24] South African Ministerial Review Commission report, p. 56; Hans Born and Ian Leigh, Making Intelligence Accountable, Oslo, Publishing House of the Parliament of Norway, 2005, pp. 16-20.

[25] Romania (footnote 2), article 42.

[26] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, a new review mechanism for the RMCP's national security activities (hereafter the Arar Commission), p. 469.

施。监督机构在聆询证人、获得文件和其他证据方面，应得到情报部门的全面合作。

14. 监督机构享有特别权力，使他们能够履行职能。具体而言，他们有权自己启动调查属于其职权范围内的情报部门的工作，允许他们接触一切必要的资料。接触资料的权力，包括阅览所有有关档案和文件的法定权力，[27] 视察情报部门的场地，[28] 和传唤情报部门的任何成员，要求其宣誓作证。[29] 这些权力有助于确保监察人员能够有效地监督情报部门的活动，全面调查可能违反法律的情况。一些国家已经采取措施，加强监督机构的调查权限，规定任何拒绝与他们合作的行为属于犯罪。[30] 这意味着监督机构可利用执法权威确保有关个人的合作。[31] 虽然较大的法律权力是有效监督的关键，但在这方面的良好做法是配合必要的人力和财力资源，以便能够充分利用这些权力，履行他们的职权。因此，很多监督机构由议会直接提供的独立的预算，[32] 能够雇用专家工作人员[33] 和聘请外部专家。[34]

做法 8. 监督机构采取一切必要措施，对工作过程中接触的机密资料和个人资料加以保护。监督机构的人员违反有关要求，将按规定给予惩罚。

15. 情报监督机构在工作过程中可能接触机密和敏感信息。因此，采取了各种办法确保监督机构和他们的工作人员不得有意或无意泄漏这些信息。首先，几乎无一例外地禁止监督机构的成员和工作人员未经授权泄漏这些信息。不遵守有关规定者，通常受到民法和/或刑罚制裁。[35] 其次，很多监督机构还要求其成员和

[27] Sweden, Act on Supervision of Certain Crime-Fighting Activities, article 4; Netherlands (footnote 20), article 73; Canada (footnote 6), section 38(c).

[28] South Africa (footnote 23), section 8(a) goes beyond the intelligence community to allowing the Inspector-General access any premises, if necessary. According to Section 8 (8)c, the Inspector-General can obtain warrants under the Criminal Procedure Act.

[29] Croatia (footnote 2), article 105; Lithuania (footnote 23), article 23.

[30] South Africa (footnote 23), section 7a.

[31] Belgium (footnote 22), article 48; The Netherlands (footnote 20), article 74.6.

[32] Belgium (footnote 22), article 66 bis.

[33] Canada (footnote 6), section 36.

[34] Concerning the assistance of external experts, see Netherlands (footnote 20), article 76; Lithuania (footnote 23), article 23 (2); Luxembourg, Law concerning the organization of the State intelligence service, article 14 (4). On having the disposition of independent legal staff and advice: United Kingdom, Joint Committee on Human Rights, 25 March 2010, paras. 110-111.

[35] Lithuania (footnote 23), article 23.4. In South Africa, the law prescribes criminal sanctions for any unauthorized disclosure by members of the parliamentary oversight body; see South Africa (footnote 23), section 7a (a); United States of America Code, General congressional oversight provisions, section 413 (d); Norway (footnote 22), article 9.

工作人员必须通过安全审查程序，方可接触机密资料。[36] 在这种方法之外，最常见的是在议会监督机构，要求其成员必须签署保密协议。[37] 但归根结蒂，正确处理监督机构经手保密资料的方法，还是取决于监督机构成员的职业道德操守。

C. 投诉和有效补救

做法 9. 认为自己的权利受到情报部门侵犯的任何个人均可向法院或监察专员、人权专员或国家人权机构等监督机构提出申诉。受到情报部门非法行动影响的个人，有权诉诸可提供有效补救的机构，补救包括为所遭受损害提供充分赔偿。

16. 普遍认为，任何限制人权的措施均必须附有适当保障，包括个人在权利受到侵犯的情况下可通过其寻求补救的独立机构。[38] 情报部门拥有一系列权力，包括监视、逮捕和拘留权，这些权力如果被滥用，就可能侵犯人权。因此，就有机构负责处理认为自己的权利受到情报部门侵犯的个人提出的申诉、并在必要情况下向侵犯人权的受害者提供有效补救。在这方面，大体上可分为两种办法。[39] 首先，国家设立一系列负责处理针对情报部门所提出申诉的非司法机构。这些机构包括：监察专员、[40] 国家人权机构、[41] 国家审计局、[42] 议会监督机构、[43] 监察长、[44] 专门情报监督机构[45] 和情报部门申诉委员会。[46] 这些机构有权接受和

[36] For example, the staff of the German Parliamentary Control Panel undergo strict security checks, Germany, Parliamentary Control Panel Act, sections 11 (1) and 12 (1).

[37] As elected representatives of the people, the members of the Parliamentary Control Panel are not obliged to undergo a vetting and clearing procedure, see Germany (footnote 36), Section 2; United States of America (footnote 35), section 413 (d).

[38] American Convention on Human Rights, article 25; Arab Charter on Human Rights, article 23; Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights, annex (E/CN.4/1984/4), article 8; European Convention for the Protection of Human Rights and Fundamental Freedoms, article 13; International Covenant on Civil and Political Rights, article 2.

[39] Hans Born and Ian Leigh, Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies, Oslo, Publishing House of the Parliament of Norway, 2005, p. 105.

[40] Netherlands (footnote 20), article 83; in Finland: with regard to data stored by the intelligence service, the Data Protection Ombudsman (reply); Greece: Ombudsman (reply); Estonia: Legal Chancellor (reply).

[41] Jordan, Law on the National Centre for Human Rights.

[42] For control of the budget of the intelligence service: Costa Rica, Organic Act of the Republic's General Audit.

[43] Romania (footnote 15), article 16.

[44] South Africa (footnote 23), section 7(7).

[45] Norway (footnote 22), article 3; Canada (footnote 6), sections 41, 42, 46 and 50.

[46] Kenya (footnote 16), articles 24-26.

调查申诉；然而，它们一般不能下达具有约束力的命令或提供补救，因此，侵犯人权的受害者需要通过法院寻求补救。第二，司法机构可接受针对情报部门的申诉。这类机构可以是专门为此目的成立的司法机构，[47] 或者是一般司法系统的一部分；它们一般都有权下令采取补救行动。

做法 10. 负责处理因情报部门的活动引起的申诉和有效补救要求的机构独立于情报部门和政务机关。这种机构可不受任何阻碍地接触一切有关信息；拥有进行调查所必要的资源和专门知识；有权下达具有约束力的命令。

17. 为使一个机构能为人权遭受侵犯提供有效补救，它必须独立于参与受到指责的活动的机构；能确保程序公正；能下达具有约束力的裁决。[48] 为此，国家向这类机构授予必要的法定权力，使其能对申诉进行调查，向情报部门侵犯人权的受害者提供补救。所授权力包括完全和不受任何阻碍地接触一切有关信息，传唤证人、获取宣誓证词的调查权力，[49] 决定与自身处理任何事项有关的程序，以及下达具有约束力的命令的权力。[50]

D. 公正和不歧视

做法 11. 情报部门开展工作的方式应有助于增进和保护在国家管辖之下的所有个人的人权和基本自由。情报部门不得以性别、种族、肤色、语言、宗教、政治或其他主张、民族或社会出身或其他地位为由歧视任何个人或群体。

18. 情报部门是国家机器的一个组成部分，应有助于保证在国家管辖之下的所有个人的人权。它们应受国际人权法律中公认的不歧视原则的约束。这一原则要求国家尊重个人的权利和自由，不带任何基于禁止理由的歧视。[51] 许多国家都将这一原则纳入了本国法律，要求其情报部门以符合国家和社会整体利益的方式执行任务。国家明确禁止情报部门为促进任何族裔、宗教、政治或其他群体的利益而行动，或为此而被利用。[52] 另外，国家还应确保其情报部门的活动(特别是

[47] United Kingdom, Regulation of Investigatory Powers Act, articles 65-70; Sierra Leone (footnote 14), articles 24-25.

[48] Iain Cameron, National security and the European Convention on Human Rights: Trends and patterns, presented at the Stockholm international symposium on national security and the European Convention on Human Rights, p. 50.

[49] Kenya (footnote 16), article 26; Sierra Leone (footnote 14), article 27.

[50] United Kingdom (footnote 47), article 68.

[51] International Covenant on Civil and Political Rights, article 26; American Convention on Human Rights, article 1; Arab Charter on Human Rights, article 3.1. For case law by the Human Rights Committee see, in particular, *Ibrahima Gueye et al. v. France* (communication No. 196/1985) and *Nicholas Toonen v. Australia* (communication 488/1992).

[52] Ottawa Principles on Anti-Terrorism and Human Rights, article 1.1.3.

在反恐情况下)，所依据的是个人的行为，而不是族裔、宗教或其他这类标准。[53] 某些国家还明确禁止其情报部门据此设立个人档案。[54]

做法 12. 国家法律禁止情报部门从事任何政治活动，或以行动促进或保护特定政治、宗教、语言、族裔、社会或经济群体的利益。

19. 情报部门被赋予的权力可能具有促进或损害特定政治群体利益的潜能。为确保情报部门保持政治中立，国家法律禁止情报部门为任何政治群体的利益服务。[55] 要承担这项义务的不仅是情报部门，也有情报部门为其服务的政务机关。一些国家还采取了禁止或限制情报部门参与政党政治的措施。这类措施的例子有：禁止情报部门雇员成为政党成员；禁止情报部门接受政党的指示或金钱，[56] 或以行动促进任何政党的利益。[57] 此外，各国还采取了一些措施保证情报部门首长的中立。例如，情报部门首长的任命要接受行政部门以外的审查；[58] 有关于情报部门首长任期的法律规定和解除其职务的理由的具体规定，以及防止向情报部门首长不适当施压的保障。[59]

做法 13. 情报部门被禁止利用权力打击合法的政治活动或结社自由、和平集会和言论自由等权利的合法行使。

20. 情报部门可采用的情报收集措施可能会干涉合法政治活动或言论、结社和集会自由权利的行使。[60] 这些权利对自由社会，包括政党、媒体和民间社会的正常运转是必不可少的。因此，一些国家采取了措施，缩小情报部门为打击(或被要求打击)从事这类活动的个人和群体可利用的余地。这类措施包括绝对禁止打击合法活动、严格限制使用情报收集措施(见办法 21)，以及保有和利用情报部

[53] Australia (footnote 3), section 17A; Ecuador (footnote 14), article 22; Canada, Macdonald Commission, p. 518.

[54] Argentina (footnote 2), article 4.

[55] Australia (footnote 3), section 11, (2A); Sierra Leone (footnote 14), article 13 (d); Romania (footnote 2), article 36.

[56] Bosnia and Herzegovina (footnote 6), article 45; Albania (footnote 21), article 11; Kenya (footnote 16), article 15 (1)a; Lithuania (footnote 9), article 24.

[57] Botswana (footnote 21), section 5(2); Sierra Leone (footnote 14), section 13 (d); United Kingdom (footnote 20), section 2 (2); South Africa (footnote 17), section 199(7).

[58] For the involvement of parliament; see Belgium (footnote 22), article 17; Australia (footnote 3), section 17(3).

[59] Poland, Internal Security Agency and Foreign Intelligence Act, Article 16; Croatia (footnote 2), article 15(2).

[60] Canada, MacDonald Commission, p. 514; South African Ministerial Review Commission, pp. 168-169, 174-175; Venice Commission (1998), p. 25.

门收集的个人资料(见做法 23)。[61] 鉴于媒体在任何社会中的重要作用，一些国家为保护记者不被情报部门打击采取了特别措施。[62]

E. 国家对情报部门的责任

做法 14. 在国际上，国家为本国情报部门、情报人员及其雇用的任何私人承包者的活动负有责任，不论活动在何处进行，也不论国际不法行为的受害者是谁。因此，行政机关要采取措施，确保全面控制其情报部门的活动并为此承担责任。

21. 根据国际法，国家对情报部门和情报人员的活动负有责任，不论他们在世界何处活动。这一责任的范围可延伸到本国雇用以从事情报工作的任何私人承包者。[63] 国家有确保其情报部门不侵犯人权以及在发生这种侵权行为的情况下提供补救的法定义务。[64] 因此，国家对其情报部门采取节制和管理措施，以促进遵守法治，特别是符合国际人权法。[65] 对情报部门实行行政控制对实现这些目的十分重要，因此，有关规定被纳入了许多国家法律。[66]

F. 个人责任与问责

做法 15. 宪法、成文法和国际法适用于情报部门成员，与适用于任何其他政府官员一样。允许情报官员采取通常会侵犯人权的行动的任何例外都受到严格限制，并在法律中有明确规定。这些例外决不允许违反国际法或国家所承担人权义务的强制性准则。

---

[61] Canada (footnote 6), section 2; Switzerland (footnote 5), article 3 (1); Japan, Act Regarding the Control of Organizations having Committed Indiscriminate Mass Murder, article 3(1)and(2); United Republic of Tanzania, Intelligence and Security Act, article 5 (2)b.

[62] Netherlands, Security and Intelligence Review Commission, Supervisory Report no. 10 on the investigation by the General Intelligence and Security Service (GISS) into the leaking of State secrets, 2006, point 11.5.

[63] Montreux document on pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict, pp. 12, 35.

[64] Croatia (footnote 2), article 87(1); Human Rights Committee, general comment no. 31 on the nature of the general legal obligations imposed on States parties to the Covenant (CCPR/C/21/Rev.1/Add.13), para. 4; Michael Defeo, “What international law controls exist or should exist on intelligence operations and their intersections with criminal justice systems?”, *Revue international de droit penal* 78, no.1 (2007), pp. 57-77; European Commission for Democracy through Law, opinion 363/2005 on the International Legal Obligations of Council of Europe Member States in Respect of Secret Detention Facilities and Inter-State Transport of Prisoners, p. 15.

[65] E/CN.4/2005/102/Add.1, Article 36.

[66] See also practice 6.

22. 虽然非常强调情报部门的法定责任，但情报部门的个人成员对其行动也同样负有责任，而且会被追究这种责任。[67] 一般而言，宪法、成文法和国际刑法均适用于情报官员，与适用于任何其他个人一样。[68] 许多国家将情报部门任何成员故意违反宪法或成文法的行动，和(或)命令或要求采取这类行动，作为追究民事责任或刑事罪责的一种理由。[69] 这种惯例可促进在情报部门内遵守法治，有助于防止有罪不罚。许多国家授权其情报部门成员从事如果由普通公民进行就构成刑事犯罪的活动。[70] 这种授权，如果有严格限制并在法律上做出规定，再加上适当保障，则不失为一种良好做法。[71] 授权情报官员采取根据国家法律通常为非法行动的法律规定，其适用范围不应扩大到违反宪法或不可减损的国际人权标准的行动。[72]

做法 16. 对情报部门任何成员或代表情报部门行动的个人违反国家法律或国际人权法或命令采取这类行动，国家法律规定了刑事、民事或其他制裁。有关法律还规定了追究个人对违法行为承担责任的程序。

23. 为确保追究情报部门雇员对任何违法行为的责任，国家规定并执行对具体犯罪行为的制裁。这有助于促进在情报部门内部遵守法治和尊重人权。节制情报部门的许多国家法律都包括了对违反这类法律或其他国家法律和国际法有关条款的雇员的具体制裁。[73] 鉴于情报部门的许多活动都是秘密进行的，(雇员的)刑事犯罪行为可能不易被有关检察机关发现。因此，一个好的做法是，国家法律要求情报部门领导向检察机关提交可能有犯罪行为的案件。[74] 在有酷刑等严重侵犯人权行为的情况下，国家有起诉情报部门成员的国际法律义务。[75] 情报部门雇

[67] ECOWAS Code of Conduct, articles 4 and 6.

[68] International Commission of Jurists, “Assessing damage, urging action”, report of the Eminent Jurists Panel on Terrorism, Counter-terrorism and Human Rights, pp. 85-89 (hereafter ICJ-EJP report); Imtiaz Fazel, “Who shall guard the guards?: civilian operational oversight and Inspector General of Intelligence”, in “To spy or not to spy? Intelligence and Democracy in South Africa”, p. 31.

[69] Morton Halperin, “Controlling the intelligence agencies”, First Principles, vol. I, No. 2, October 1975.

[70] United Kingdom (footnote 47), articles 1, 4; United Kingdom (footnote 20), section 7. With regard to engaging in criminal activities as part of intelligence collection, see Netherlands (footnote 20), article 21 (3); United Kingdom (footnote 47), articles 1, 4; United Kingdom (footnote 20), section 7.

[71] South African Ministerial Review Commission, pp. 157-158.

[72] Netherlands (footnote 20), annex.

[73] Croatia (footnote 2), articles 88-92; Romania (footnote 15), articles 20-22, Argentina (footnote 2), article 42; Bulgaria (footnote 15), article 88(1), 90 & 91; South Africa (footnote 23), articles 18, 26.

[74] Canada (footnote 6), section 20 (2-4).

[75] Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, articles 4 and 6.

员的刑事责任不仅产生于其对有关活动的直接参与，也产生于其关于进行有关活动的命令或同谋关系。[76]

做法 17. 情报部门成员有拒绝执行会违反国家法律或国际人权法的上级命令的法律义务。向在这种情况下拒绝执行命令的情报部门成员提供适当保护。

24. 国家法律要求情报部门成员拒绝执行他们认为会违反国家法律或国际人权法的命令，这是一种良好做法。[77] 虽然这种规定更常见于节制武装部队的法律中，但一些国家也将其纳入了本国节制情报部门的法律。[78] 让情报部门成员拒绝执行非法命令的要求，是防止对人权的可能侵犯以及防止有关政府命令情报部门采取行动以促进或保护其自身利益的一项重要保障。一项既定的国际法原则是，对于因按照上级要求采取行动而严重侵犯人权的个人，不免除其刑事责任。[79] 因此，为避免个人刑事责任，情报部门成员被要求拒绝执行其应知道明显违法的任何命令。这就说明了对情报官员进行人权培训的重要性，因为他们需要了解根据国际法他们应有的权利和义务(见做法 19)。为创造一种不容忍侵犯人权行为的环境，国家规定了对拒绝执行违法命令的情报部门成员的保护，以防止他们遭受报复。[80] 拒绝执行违法命令的义务与是否有某种内部和外部机制密切相关，通过这种机制，情报部门雇员可表明他们对违法命令的关切(见做法 18)。

做法 18. 情报部门成员可利用内部程序报告违法情况。辅助这些程序的是一个独立机构，它有权接触进行全面调查所必要的一切资料，并在内部程序不足以解决问题的情况下采取行动对违法情况给予补救。出于善意报告违法情况的情报部门成员受到可令其避免遭受任何报复的法律保护。这种保护的范围可延伸到向媒体或广大公众披露情况(在被迫作为最后手段，事关公众严重关切问题的情况下)。

25. 就发现侵犯人权行为、财务舞弊和其他违法行为等情报部门内部的违法情况而言，情报部门雇员时常处于最直接和最好的位置。因此，在国家法律中为情报部门成员举报违法情况规定出具体程序，是一种良好做法。[81] 这类规定旨在鼓励情报部门成员举报违法行为，同时确保对可能比较敏感的情况的披露和调查

[76] Rome Statute, article 25 (3) (b-d), Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, article 1.

[77] Hungary, Act on the National Security Services, section 27; Lithuania (footnote 9), article 18; ECOWAS Code of Conduct, article 16.

[78] Bosnia and Herzegovina (footnote 6), article 42; South Africa (footnote 23), article 11 (1).

[79] Rome Statute, article 33; Geneva Conventions I-IV; Commission on Human Rights (footnote 65), principle 27; see also Lithuania (footnote 9), article 18.

[80] Bosnia and Herzegovina (footnote 6), article 42.

[81] New Zealand, Protected Disclosures Act, section 12; Bosnia and Herzegovina (footnote 6), article 42; Canada, Security of Information Act, section 15.

有控制地进行。国家做法表明，这种披露有几种渠道，包括负责接收和调查情报部门成员所披露情况的内部机制、[82] 负责接收和调查披露情况的外部机构以及直接向这些机构披露情况的情报部门成员。[83] 在某些系统中，如果内部机构不能适当解决情报部门成员关切的问题，他们就只能去找外部机构。[84] 在某些国家，允许情报部门成员作为最后手段公开披露情况，或公开披露特别是涉及生命威胁等严重问题的情况。[85] 不论披露渠道的具体性质如何，在国家法律中规定向依法披露情况的个人提供保护，使其免受报复，这都是一种良好做法。[86]

G. 专业水准

做法 19. 情报部门及其监督机构采取措施，培养崇尚职业精神、尊重法治和人权的机构文化。尤其是，情报部门负责对其成员进行关于国家法律和国际法，包括国际人权法中有关规定的培训。

26. 情报部门的机构文化是指广大雇员共有的主要价值观、态度和习惯做法。它是决定情报官员对法治和人权的态度的主要因素之一。[87] 的确，只是法律和体制框架不能确保情报部门成员尊重人权和法治。一些国家和它们的情报部门制定了道德准则或职业原则，以培养一种珍视和崇尚尊重人权和法治的文化。[88]

---

[82] United Kingdom, Intelligence and Security Committee, annual report 2007-2008, paras. 66-67 (reference to the position of an "ethical counsellor" within the British Security Service); United States of America, Department of Justice, Whistleblower Protection for Federal Bureau of Investigation Employees, Federal Register, vol. 64, No. 210 (Inspector General and the Office of Professional Responsibility).

[83] Germany (footnote 36), section 8(1); New Zealand (footnote 81), section 12. It should be noted that, in New Zealand, the Inspector-General is the only designated channel for protected disclosures.

[84] United States of America (footnote 35), title 50, section 403(q), 5; Canada (footnote 6), section 15 (5); Australia, Inspector-General of Intelligence and Security Act 1986, sections 8 (1)a,(2)a,(3)a and 9(5).

[85] Canada (footnote 81), section 15; Germany, Criminal Code, sections 93(2), 97a and 97b. The importance of public disclosures as a last resort was also highlighted in the report "Whistleblower protection: a comprehensive scheme for the Commonwealth public sector" House of Representatives Standing Committee on Legal and Constitutional Affaires on the inquiry ino whistleblowing protection within the Australian Government public sector, pp. 163-164; see also National Commission on Terrorist Attacks Upon the United States, "The 911 Commission Report", chapter 3.

[86] Netherlands, Government Decree of 15 December 2009 Laying Down a Procedure for Reporting Suspected Abuses in the Police and Government Sectors, article 2; United States of America, title 5, US Code, section 2303(a); Bosnia and Herzegovina (footnote 6), article 42; Australia (footnote footnote 84), section 33; Parliamentary Assembly of the Council of Europe, Draft Resolution on the protection of whistleblowers, doc. 12006, paras. 6.2.2 and 6.2.5.

[87] South African Ministerial Review Commission on Intelligence, p. 233.

[88] South Africa, Five principles of intelligence service professionalism, South African Intelligence Services; South Africa, Ministerial Regulations of the Intelligence Services, chapter 1(3)(d), 1(4)(d); see also Bulgaria (footnote 15), article 66 (with regard to application of the Ethical Code of Behaviour for Civil Servants to members of the intelligence services).

行为准则通常包括适用于所有情报人员的有关适当行为、纪律及道德标准的规定。[89] 在某些国家，由负责情报工作的部长负责颁布这类文件；这就保证了对其内容的政治责任。[90] 将行为准则置于内部和外部监督机构的监督和审查之下，是一种良好做法。[91] 培训是在情报部门培养职业机构文化的另一个重要手段。许多情报部门推行了强调职业精神的培训方案，对雇员进行有关宪法标准、成文法和国际人权法的教育。[92] 推行培训方案既是法律要求又受法律节制，同时涵盖所有(未来的)情报部门成员。[93] 最后，可通过奖励道德和职业行为的内部人事管理政策加强职业文化。

H. 人权保障

做法 20. 情报部门采取的任何限制人权和基本自由的措施必须符合下列条件：

(a) 符合国际人权标准的公开规定的法律；

(b) 所有这些措施必须是为履行其法定职责的情报部门所绝对必要的；

(c) 采取的措施必须与其目标相称。这就要求，情报部门选择对人权的限制最轻微的措施，并采取特别照顾，以尽量减少任何措施对个人、其中尤其包括不涉嫌任何不法行为的人的不良影响；

(d) 情报部门采取的任何措施不得违反国际法强制性规范或任何人权的本质；

(e) 对于限制人权的任何措施的使用有一个明确和全面的授权、监督和监视制度；

(f) 其权利可能受到情报部门限制的人能够向独立机构投诉并寻求有效的补救。

27. 根据国家法律，大部分情报部门被允许从事限制人权的活动。这些权力主要在于情报的搜集方面，但也包括执法措施、个人资料的使用和个人信息的共享。国家法律载述对人权的保障，主要有两个原因：首先，把对个人权利的干预

[89] United Republic of Tanzania (footnote 61), article 8(3); South Africa, Five principles of intelligence service professionalism, South African Intelligence Services.

[90] United Republic of Tanzania (footnote 61), article 8(3).

[91] Netherlands, Supervisory Committee on Intelligence and Security Services, On the Supervisory Committee's investigation into the deployment by the GISS of informers and agents, especially abroad, see section 4; for the role of Inspectors-General in these matters, see South African Ministerial Review Commission, p. 234.

[92] South African Ministerial Review Commission on Intelligence, pp. 209 and 211.

[93] Argentina (footnote 2), articles 26-30; South Africa (footnote 23), article 5(2)(a).

限制在根据国际人权法能够允许的范围，其次，防止这些措施的任意或不受约束的使用。[94]

(a) 限制人权的任何措施，必须以符合国际人权法标准、在使用该措施的时候正式生效的一项法律予以规定。[95] 这样的法律以狭义和精确的术语概述上述措施，确定使用这些措施的严格条件，并规定其使用必须与情报部门的任务直接有关。[96]

(b) 许多国家的法律还规定："限制人权的情报措施，必须是一个民主社会所需要的。[97] 必要性包括任何措施的使用明确和合理地与国家法律所规定的保护合法的国家安全利益有关。[98]

(c) 相称性原则载于许多国家的法律，并规定限制人权的任何措施必须与指定的(和法律允许的)目标相称。[99] 为了确保情报部门采取的措施是相称的，许多国家要求"其情报部门用尽可能最不侵扰的手段达到给定的目标。[100]

(d) 通过国家的法律，情报部门被禁止使用会违反国际人权标准和/或国际法强制性规范的任何措施。一些国家在其情报部门法中明确禁止严重侵犯人权行为。[101] 虽然可将不可减损的人权单独列出，视为不可侵犯的人权，但每项人权都包含一个不容限定的核心内容。

(e) 各国确保限制人权的情报措施均受制于法律规定的核准程序，以及事后的监督和审查(见做法 6-7、21-22、28、32)。

(f) 国际人权法的一项基本要求是，侵犯人权行为的受害者可以寻求补救和救济。许多国家已制订程序，以确保个人可以要求一个独立的机构就这种要求作出裁决。[102] (见做法 9-10)。

---

[94] Siracusa Principles (footnote 38).

[95] See practices nos. 3 and 4; Croatia (footnote 2), article 33; Lithuania (footnote 9), article 5; Council of Europe (footnote 4), para. 5.

[96] MacDonald Commission, p. 423; Morton Halperin (footnote 69).

[97] Sierra Leone (footnote 14), article 22 (b); United Republic of Tanzania (footnote 61), article 14 (1); Japan (footnote 61), article 3(1); Botswana (footnote 21), section 22(4) a-b.

[98] Johannesburg Principles on National Security, Freedom of Expression and Access to Information, principle 2(b); Ottawa Principles, principle 7.4.1.

[99] Germany (footnote 2), section 8(5); Germany, Act on the Federal Intelligence Service, section 2(4); Council of Europe (footnote 4), article V (ii); MacDonald Commission report, p. 513.

[100] Croatia (footnote 2), article 33(2); Hungary (footnote 77), section 53(2); United States of America, Executive Order No. 12333, section 2.4. Federal Register vol. 40, No. 235, section 2; Germany (footnote 2), Section 8(5); Germany (footnote 99), Section 2(4); A/HRC/13/37, paras. 17 (f) and 49.

[101] Botswana (footnote 21), section 16 (1)(b)(i) related to the prohibition of torture and similar treatment.

[102] American Convention on Human Rights, article 25; Arab Charter, article 9; Siracusa principles, article 8; European Court of Human Rights, *Klass v. Germany*, A 28 (1979-80), 2 EHHR 214, para. 69. See also practices 9 and10.

I. 情报收集

做法 21. 国家法律概述了情报部门可使用的收集措施种类；可允许的情报收集目标；可被收集情报的人员和活动类别；能证明收集措施的使用有正当性的怀疑阀值；对可使用收集措施之期限的限制；以及对情报搜集措施之使用的授权、监督和审查程序。

28. 在大多数国家，情报部门可采取强制措施，例如秘密监视和截取通讯，以便为履行任务收集必要的资料。法治的基本要求是，个人必须知道公共机关可用以限制其权利的措施，并且能够预知哪些活动可能引起这些措施的使用。[103] 国家法律概述了可能被收集情报的人员和活动的类别，[104] 以及开始采取特定措施所需要的怀疑阀值。[105] 有些国家的法律还规定对特定类别的个人，尤其是记者和律师使用侵入收集措施的限制。[106] 这些保护措施的目的，是保护那些被认为对自由社会的运作不可或缺的专业特权，例如新闻记者有不透露其消息来源的权利，或律师与客户的关系。对使用侵入收集方法的严格限制有助于确保情报的搜集是必要的，并且只限于可能涉及对国家安全构成威胁的个人和团体之活动。国家法律还包括对可使用侵入收集措施之期限的准则，过期之后，情报部门必须寻求重新授权，以便继续加以使用。[107] 同样，好的做法是由国家法律规定，一旦情报收集措施的使用已经完成任务，或者明显地无法达到目的，立即予以停止。[108] 这些规定有助于尽量减少对当事人权利的侵犯，并且帮助确保情报收集措施符合相称的要求。

---

[103] European Court of Human Rights, *Liberty v. UK*, para 63; *Malone v. The United Kingdom*, 2 August 1984, para.67; Council of Europe (footnote 4), article V (i*); Huvig v. France*, para. 32; Kenya (footnote 16), article 22 (4); Romania (footnote 8), article 20. This recommendation is also made in the Moroccan TRC Report, vol. 1, chap. IV, 8-4; Hungary (footnote 77), sections 54, 56; Croatia (footnote 2), article 33 (3-6).

[104] European Court of Human Rights, *Weber & Saravia v. Germany*, decision on admissibility, para. 95; European Court of Human Rights, *Huvig v France*, 24 April 1990, para. 34; United Republic of Tanzania (footnote 61), article 15(1).

[105] Kenya (footnote 16), article 22 (1); Sierra Leone (footnote 14), article 22; Tanzania (footnote 61), article 14 (1), 15 (1); Canada (footnote 6), section 21 (all reasonable grounds); Netherlands (footnote 20), article 6(a) (serious suspicion); Germany (footnote 2), section 9(2); Germany, Constitutional Court, Judgement on Provisions in North-Rhine Westphalia Constitution Protection Act, 27 February 2008.

[106] Germany, G10 Act, section 3b; Germany (footnote 85), sections 53 and 53a.

[107] Germany (footnote 106), section 10 (5); Kenya (footnote 16), article 22 (6); Romania (footnote 8), article 21(10); South Africa (footnote 23), section 11(3)a; Croatia (footnote 2), article 37; Canada (footnote 6), section 21 (5); Hungary (footnote 77), section 58(4), Section 60 (termination); European Court of Human Rights, *Weber & Saravia v. Germany*, para. 95.

[108] United Kingdom (footnote 47), section 9; Germany (footnote 106), section 11(2); Germany (footnote 2), section 9 (1); European Court of Human Rights, *Huvig v France*, para. 34.

做法 22. 要求大大限制人权的搜集情报措施至少由该情报部门以外的一个独立的监督机构予以授权和监督。这个机构有权责令修改、暂停或终止这种收集措施。对人权施加重大限制的情报收集措施需要经过多层次的授权过程，包括情报部门内部、政务部门、情报部门以外独立机构以及行政机关的批准。

29. 国家法律的普遍做法包括详细规定对限制人权的所有情报收集措施的授权过程。[109] 授权程序规定情报部门必须证明按照一个明确的法律框架采取建议的情报收集措施的正当性(见做法 20 和 21)。这是确保收集措施依法使用的关键机制。侵入收集措施的良好做法是由一个独立于情报部门的机构，即承担政治责任的执政成员[110] 或(准)司法机关予以认可。[111] 司法机构是独立于情报过程的，因此最适合由它们对使用侵入收集权力的申请进行独立和公正评估。[112] 此外，让最具侵扰性质的情报收集方法(例如通讯内容的截取、邮件的拦截、和诡异地侵入财产)的授权者包括情报部门的高级管理人员、担任政治责任的行政官员、和(准)司法机关，显然是良好的做法。[113]

30. 国家还保证，情报的收集持续由情报部门以外的机关予以监督。良好的做法是要求情报部门报告持续使用的收集措施和让外部监督机构有权下令终止收集措施。[114] 在许多国家，外部监督机构也对情报收集措施的使用进行事后监督，以确定其使用是否获得授权，并且符合法律规定。[115] 这一点特别重要，因为其权利受到情报收集之影响的个人不可能知道，因此，挑战其合法性的机会受到限制。

---

[109] Germany (footnote 106), sections 9-10; Canada (footnote 6), section 21; Netherlands (footnote 20), articles 20(4) and 25(4); Kenya (footnote 16), article 22.

[110] Australia (footnote 3), articles 25, 25a; Netherlands (footnote 20), articles 19, 20(3-4), 22 (4), 25; United Kingdom (footnote 47), sections 5-7.

[111] Argentina (footnote 2), articles 18 and 19; Kenya (footnote 16), article 22; Sierra Leone (footnote 14), article 22; Croatia (footnote 2), articles 36-38; Romania (footnote 8), articles 21 and 22; Canada (footnote 6), section 21 (1-2); South Africa (footnote 23), section 11. See also European Court of Human Rights, *Klass v. Germany* (footnote 102), para. 56.

[112] The European Court of Human Rights has indicated its preference for judicial control for the use of intrusive collection methods, see *Klass v. Germany* (footnote 102), paras. 55-56. See also Parliamentary Assembly of the Council of Europe, recommendation 1402, ii. The South African Ministerial Review Commission argues that all intrusive methods should require judicial authorizations; see p. 175; Cameron (footnote 48), pp. 151, 156-158.

[113] Canada (footnote 6), section 21; Germany (footnote 106), sections 9-11 and 15(5). See also Canada, MacDonald Commission, pp. 516-528.

[114] Croatia (footnote 2), article 38 (2); United Kingdom (footnote 47), section 9(3-4); Germany (footnote 106), section 12 (6). See also Canada, MacDonald Commission, p. 522.

[115] United Kingdom (footnote 47), section 57(2); Norway, Parliamentary Intelligence Oversight Committee; Netherlands (footnote 20), article 64(2)(a).

J. 个人资料的管理和使用

做法 23. 公开提供的法律概述情报部门可以持有哪些个人数据，这种数据的使用、保存、删除和披露适用哪些标准。情报部门被允许保留为了履行其任务绝对必要的个人资料。

31. 有若干一般性原则适用于对个人数据的保护，通常载于国家法律[116]，以及国际文书。[117] 这些包括下列要求：以合法和公正的方式收集和处理个人资料；对个人数据的使用受到限制，仅限于原来的指定用途；采取步骤，以确保个人数据的记录准确；不再需要该个人资料时，即予以删除；个人有权查阅和改正其个人资料文件。[118] 在情报部门使用个人资料的情形下，个人资料文件的开放、保留和处理会对人权产生严重的影响。因此，情报部门对个人资料的管理和使用准则载列于公共法定法。这是使行政或情报部门不致对这些事项有不受制衡的权力的法律保障。[119] 第二项保障是：制定法律准则，具体规定和限制情报部门打开和保持个人数据档案的理由。[120] 第三，各国的惯例是：情报部门向一般公众通报由情报部门保存的个人资料的类型；这包括可能被保留的个人资料的类型和范围，以及由情报部门保留个人资料的可以允许的理由。[121] 第四，各国已经将情报人员既定的法律框架以外透露或使用个人资料规定为刑事罪行。[122] 最后一个保障是，国家明确规定，情报部门不得基于歧视性的理由存放个人资料。[123]

---

[116] Japan, Act on the Protection of Personal Information held by Administrative organs; Switzerland, Loi fédérale sur la protection des données.

[117] A/HRC/13/37, paras. 11-13. For specific examples of international principles, see the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108); the Organization for Economic Cooperation and Development, Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); The Guidelines for the Regulation of Computerized Personal data Files (General Assembly resolution 45/95 and E/CN.4/1990/72).

[118] It should be acknowledged that international agreements permit derogation from basic principles for data protection when such derogation is provided for by law and constitutes a necessity in the interest of, inter alia, national security. See Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), article 9.

[119] European Court of Human Rights, *Weber and Saravia v. Germany*, no. 54934/00, 29 June 2006, paras. 93-95.

[120] MacDonald Inquiry, p. 519; Netherlands (footnote 20), article 13.

[121] Canada, Privacy Act, section 10. An overview of personal information banks maintained by the Canadian Security and Intelligence Services can be found on the website of the Government of Canada (http://www.infosource.gc.ca/inst/csi/fed07-eng.asp).

[122] Romania (footnote 15), article 21.

[123] For example, in Ecuador, intelligence services are not allowed to store personal data on the basis of ethnicity, sexual orientation, religious belief, political position or of adherence to or membership in political, social, union, communitarian, cooperative, welfare, cultural or labour organizations; see Ecuador (footnote 15), article 22.

做法 24. 情报部门对其所持有的个人资料的相关性和准确性进行定期评估。情报部门必须依照法律删除或更新已经被评估为不准确、或不再与其任务、监督机构的工作或可能的法律程序有关的任何资料。

32. 各国已经采取步骤，以确保情报部门定期检查其职权范围内的个人资料档案是否准确和具有相关性。[124] 关于个人资料的相关性和准确性的保障有助于确保对隐私权的持续侵犯减少到最低限度。在一些国家，情报部门不仅有义务销毁不再相关的文件，[125] 也应销毁不正确、或被错误处理的文件。[126] 尽管情报部门通常必须删除不再与其任务有关的数据，但重要的是，这样做不得对监督机构的工作或可能的司法诉讼产生不利影响。情报部门持有的信息可能对有关个人有重大影响的法律诉讼构成证据，这类材料的可得性对于保证正当程序权利可能是重要的。因此，良好的做法是：情报部门必须保留可能导致法律诉讼的所有案件记录(包括原始单据和业务票据)，而任何此类资料删除应由一个外部机构监督(见做法 25)。[127]

做法 25. 由一个独立的机构来监督情报部门对个人资料的使用。这个机构能够取得情报部门持有的所有文件，并有权下令披露有关个人的资料，以及销毁其中所载的文件或个人资料。

33. 在许多国家，个人资料文件的管理由独立机构进行定期和持续的监督。[128] 这些机构的任务是对当前和过去业务的个人资料文件进行定期视察，以及抽查。[129] 国家还规定由独立的监督机构检查关于文件管理的内部指示是否遵守法律。[130] 各国承认，监督机构必须能够决定它自己的工作/检查方法，并且有足够的资源和能力就情报部门对个人资料的管理和使用进行定期检查。[131] 情报部门有与负责审议个人资料的管理和使用的监督机构充分合作的法律责任。[132]

---

[124] Germany (footnote 2), section 14 (2); Germany (footnote 106), section 4 (1), section (5); Switzerland (footnote 5), article 15 (1) (5).

[125] Germany (footnote 2), section 12 (2); Kenya (footnote 16), section 28(1).

[126] Netherlands (footnote 20), article 43; Croatia (footnote 2), article 41(1).

[127] *Charkaoui v. Canada* (Citizenship and Immigration), [2008] 2 S.C.R. 326, 2008 SCC 38, para. 64.

[128] Sweden (footnote 27), article 1; Hungary (footnote 77), section 52. See also practices 6-8.

[129] In Norway, the Parliamentary Intelligence Oversight Commission is obliged to carry out six inspections per year of the Norwegian Police Security Service, involving at least 10 random checks in archives in each inspection and a review of all current surveillance cases at least twice per year; see Norway, Instructions for monitoring of intelligence, surveillance and security services, articles 11.1 (c) and 11.2 (d).

[130] See Germany (footnote 2), section 14 (1), according to which the Federal Commissioner for Data Protection and Freedom of Information should be heard prior to issuing a directive on file management.

[131] Sweden, Ordinance containing Instructions for the Swedish Commission on Security and Integrity Protection, paras. 4-8 (on management and decision-making), 12 and 13 (on resources and support).

[132] Hungary (footnote 77), section 52.

做法 26. 个人有可能要求查阅由情报部门持有的个人资料。个人可以向有关当局提出申请，或通过一个独立的资料保护或监督机构来行使这一权利。个人有权纠正在个人资料中的不准确之处。这些一般性规则的任何例外情况由法律予以规定和严格限制、符合比例原则和情报部门履行其任务的需要。情报部门必须向一个独立的监督机构证明它不发布个人信息的任何决定具有正当理由。

34. 许多国家赋予个人查阅由情报部门持有的个人资料的权利。这项权利的行使可以向情报部门、[133] 有关部长 [134] 或一个独立监督机构提出申请。[135] 个人查阅其个人资料文件的权利应在保障隐私权和获取信息自由的情况下予以理解。这项保障之所以重要，不仅因为它使个人能够检查其个人资料文件是否准确、合法，还因为它可以防止滥用、管理不善和腐败。事实上，个人查阅情报部门持有的个人资料的权利，有助于提高情报部门决策过程的透明度和问责制，从而有助于培养公民对政府行为的信任。[136] 有些国家可能会基于一些理由限制查阅个人资料文件，例如维护正在进行的调查和保护情报部门的情报来源和方法。但是，良好的做法是在法律上概要叙述这种限制，以及满足相称性和必要性的要求。[137]

K. 逮捕和羁押权的行使

做法 27. 情报部门未经授权不能履行执法职能，则不准许行使逮捕和拘留权。如果与负责处理同类活动的执法机构权力重叠，则不授予情报部门逮捕和拘留权。

35. 广泛公认的良好做法是，如果情报部门的法定任务不要求其对威胁国家安全罪，比如恐怖主义，履行执法职能，则明确禁止其行使逮捕和拘留权。[138] 存在着反对合并情报和执法职能的强烈理由。[139] 然而，如果国家法律授予情报部

[133] Croatia (footnote 2), article 40 (1).

[134] Netherlands (footnote 20), article 47.

[135] Sweden (footnote 27), article 3; Switzerland (footnote 5), article 18 (1).

[136] David Banisar, Public oversight and national security: Comparative approaches to freedom of information, Marina Caparini and Hans Born (eds.), Democratic control of intelligence services: Containing the rogue elephant, p. 217.

[137] Netherlands (footnote 20), articles 53-56; Croatia (footnote 2), article 40 (2) (3); Germany (footnote 2), section 15(2).

[138] Albania (footnote 21), art. 9; United Republic of Tanzania (footnote 61), art. 4 (2)a; Argentina (footnote 2), art. 4 (1); New Zealand (footnote 8), sect. 4(2); Germany (footnote 2), art. 2(1).

[139] A/HRC/10/3, paras. 31, 69; Secretary-General of the Council of Europe, report under art. 52 of the European Convention of Human Rights on the question of secret detention and transport of detainees suspected of terrorist acts, notably by or at the instigation of foreign agencies, SG/Inf (2006) 5, para. 41; Parliamentary Assembly of the Council of Europe, recommendation 1402, paras. 5–6; International Commission of Jurists, “Assessing damage, urging action”, pp. 73–78, 89; Canada, MacDonald Commission, pp. 422–423 and 613–614.

门逮捕和拘留权，则良好做法是明确限于授其负责特定威胁国家安全行为，比如恐怖主义的执法职能任务范围之内。[140] 如果国家或区域执法机构有任务对威胁国家安全罪执行刑法，则没有合法理由让情报部门另外对同类活动行使逮捕和拘留权。这存在着演变出并行执法制度的危险，从而让情报部门行使逮捕和拘留权，以规避那些适用于执法机构的法律保障和监督。[141]

做法 28. 如果情报部门有逮捕和拘留权，则应依据公开的法律。行使这些权力限于合理怀疑某人已经或行将实施具体犯罪的情况。不准许情报部门仅为搜集情报而剥夺个人自由。情报部门行使任何逮捕和拘留权，应与执法机构行使这些权力一样，须受到同等程度的监督，包括对任何剥夺自由行为的合法性进行司法审查。

36. 如果授予情报部门逮捕和拘留权，则国家法律规定这类权力的目的及其可行使的条件。[142] 良好做法是：这些权力的行使严格限于合理怀疑某一犯罪(属于情报部门的任务范围之内)已经或行将实施的情况。因此不准许情报部门仅为搜集情报而行使这些权力。[143] 如果不能合理怀疑有人已经实施或将要实施某一犯罪，或者存在其他国际公认的拘留理由，则根据国际人权法不得予以逮捕和拘留。[144] 如果国家法律准许情报部门逮捕和拘留个人，则良好做法是行使这些权力受制于执法机构行使这些权力时适用的同样监督标准。[145] 最重要的是，国际人权法要求个人有权在法庭上质疑对其拘留的合法性。[146]

做法 29. 如果情报部门有逮捕和拘留权，则须遵守关于自由和公平审判权，以及禁止酷刑、不人道和有辱人格待遇等国际人权标准。情报部门行使这些权力时，必须遵守《联合国保护所有遭受任何形式拘留或监禁的人的原则》、《联合国执法人员行为守则》和《执法人员使用武力和火器的基本原则》等文书所规定的国际标准。

---

[140] Norway, Criminal Procedure Act.

[141] International Commission of Jurists, “Assessing damage, urging action”, pp. 73–78.

[142] Hungary (footnote 77), art. 32; Bulgaria (footnote 15), arts. 121(2)3, 125 and 128; Norway (footnote 140), sects. 171–190.

[143] Norway, Criminal Procedure Act (footnote 140), sects. 171–173 (implied); Hungary (footnote 77), art. 32 (implied); Lithuania (footnote 9), art. 18 (implied); Switzerland (footnote 5), art. 14 (3).

[144] Venice Commission (1998), sect. E.

[145] Cyprus, Reply; Norway (footnote 140), sects. 183–185; Bulgaria (footnote 15), art. 125(5); Mexico, reply.

[146] International Covenant on Civil and Political Rights, art. 9(4); OSCE-ODIHR, Countering Terrorism, Protecting Human Rights, pp. 158–160; Arab Charter on Human Rights, art. 8; American Convention on Human Rights, art. 7(6); Council of Europe (footnote 4), arts. VII (3) and VIII; General Assembly resolution A/RES/43/173, annex, principle 4.

37. 如果授予情报部门逮捕和拘留权，则要求其遵守关于剥夺自由的国际标准(也见做法 28)。[147] 一些国际和区域性执法官员行为守则都进一步阐述了这些标准，编纂了一系列可适用于拥有逮捕和拘留权的情报部门的良好做法。[148] 除了做法 28 概述的法律义务(对拘留进行司法审查)，还有三套标准适用于情报部门行使逮捕和拘留权。第一，绝对禁止情报部门使用酷刑、不人道和有辱人格待遇。[149] 第二，如果在逮捕和拘留过程中使用任何武力，则必须遵守国际标准，包括任何使用武力必须绝对必要、与可见的危险相称并正确报告等要求。[150] 最后，良好做法是情报部门遵守以下逮捕和拘留个人的国际标准：从逮捕之时开始记录所有逮捕、拘留和审讯情况，[151] 行使逮捕的官员向有关个人出示他们的身份并通知其被捕/拘留的原因和法律依据，[152] 被情报部门拘留的人能够有律师代理。[153]

做法 30. 不准许情报部门自行开设拘留设施，或使用第三方开设的任何秘密拘留设施。

38. 良好做法是国家法律明确禁止情报部门开设自己的拘留设施。[154] 如果准许情报部门行使逮捕和拘留权，则由执法机构管理的正规拘留中心羁押有关个人。[155] 同样，不准许情报部门使用第三方，如私人承包商经营的秘密拘留设施。这些是基本的保障，以防止情报部门任意拘留和/或可能演变出一个并行拘留制度，可在不符合国际拘留和正当程序标准的条件下羁押个人。

147 Venice Commission (1998), sect. E.

148 See Code of Conduct for Law Enforcement Officials in General Assembly resolution 34/169; Basic Principles on the Use of Force and Firearms by Law Enforcement Officials; General Assembly resolution 43/173, annex. See also Committee of Ministers of the Council of Europe, European Code of Police Ethics, recommendation (2001)10 (hereafter, European Code of Police Ethics).

149 Convention against Torture, art. 1; African Charter on Human and People's Rights, art. 5; Code of Conduct for Law Enforcement Officials, art. 5; European Code of Police Ethics, arts. 35 and 36; Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment, principle 6.

150 Code of Conduct for Law Enforcement Officials, art. 3; European Code of Police Ethics, art. 37; Council of Europe (footnote 4), art. VI (2); Morocco, IER Report, vol. 1, chap. IV, 8–6.

151 Bulgaria (footnote 15), art. 125 (8); OSCE Guidebook on Democratic Policing, 2008, arts 55–64; Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment, principle 12.

152 American Convention on Human Rights, art. 7(4); European Convention on Human Rights, art. 5(2); European Code of Police Ethics, art. 45; Council of Europe (footnote 4), art. VII (1); OSCE-ODIHR, Countering Terrorism, Protecting Human Rights, p. 157; *Fox, Campbell and Hartley v. UK*, para. 40; Norway (footnote 140), sect. 177.

153 See also European Code of Police Ethics, arts. 48, 50, 54, 55 and 57; Bulgaria (footnote 15), art. 125(6); and Norway (footnote 140), sect. 186.

154 Romania (footnote 2), art. 13.

155 Australia (footnote 3), sect. 34G(3)(i)(iii); Lithuania (footnote 9), art. 19(4); Venice Commission (1998), sect. E.

L. 情报共享和合作

做法 31. 同一国情报机构之间和与外国任何当局之间的情报共享必须根据国家法律，对情报交换，包括资料共享必须满足的条件、可与之共享情报的实体，以及适用于情报交换的安全保障等作出明确的限制规定。

39. 良好做法是情报部门之间和与本国或外国其他实体之间的所有形式资料交换在国家法律上有明确根据。国家法律载有关于情报可共享的目的、可共享情报的实体以及适用于情报共享的程序保障等标准。[156] 情报共享的法律依据是法治的一项重要要求，而对于交换个人资料尤为重要，因为这直接侵犯隐私权并可能影响一系列其他权利和基本自由。除了确保情报共享是依据国家法律，公认的良好做法是依据各方之间符合国家法律所定准则的书面协议或备忘录而共享情报。[157] 这类协议的内容通常包括：关于使用共享资料的规则、各方遵守人权和资料保护的声明，以及提供部门可请求获得关于使用共享资料的反馈的条款。[158] 情报共享协议有助于建立相互同意的关于共享资料的标准和期望，并缩小监督机构不易审查的非正式情报共享范围。

做法 32. 国家法律规定批准情报共享协议和个案情报共享的程序。任何与外国实体的情报共享协议以及可能严重影响人权的情报共享，都必须得到行政部门的批准。

40. 良好做法是国家法律为批准个案资料提供以及为达成情报共享协议而规定准则。[159] 这是为确保存在着关于情报共享责任的确定渠道，并且能够追究相关个人就之所作任何决定的责任。在许多国家，国内一级的常规情报共享由情报部门内部授权。然而，如果情报部门分享的资料可用于法庭诉讼，则良好做法是需要行政授权；在这类诉讼中使用情报可能对有关个人权利以及情报部门的活动产生深远影响。[160] 另外，许多国家法律规定，与外国实体共享情报或达成共享协议需要行政授权。[161]

---

[156] Croatia (footnote 2), arts. 58, 60; Switzerland (footnote 5), art. 17; Netherlands (footnote 20), arts. 37, 41 and 42, 58–63; Albania (footnote 21), art. 19; Canada (footnote 6), arts. 17, 19; Germany (footnote 2), sects. 19, 20, Germany (footnote 99), sect. 9; Germany (footnote 106), sects. 4 (4–6), 7 , 7a, 8 (6); Hungary (footnote 77), sects. 40, 44, 45. See also Canada, MacDonald Commission Report, p. 1080.

[157] Canada, Arar Commission, pp. 321–322; Venice Commission (2007), p. 182.

[158] Canada, Arar Commission, p. 339; Germany (footnote 2), sect. 19; Germany (footnote 106), sect. 7a(4); Netherlands (footnote 20), arts. 37, 59; Croatia (footnote 2), art. 60 (3).

[159] Croatia (footnote 2), art. 59(2); United Republic of Tanzania (footnote 61), art. 15 (3) (4); Canada (footnote 6), art. 17.

[160] Netherlands (footnote 20), arts. 38.1 and 61; Canada (footnote 6), art. 17.1 (a).

[161] Netherlands (footnote 20), art. 59 (5–6); Croatia (footnote 2), art. 59(2); United Kingdom, Intelligence and Security Committee, p. 54; Canada (footnote 6), art. 17.1 (b); Germany (footnote 106), art. 7a; Germany (footnote 2), sect. 19(1).

做法 33. 在缔结任何情报共享协议或个案共享情报时，情报部门评估对方的人权和资料保护记录，以及关于对方的法律保障和机构管理。情报部门在交付资料前，确定是否任何共享情报与接受方的任务有关、将根据所附条件而使用，并且不用于侵犯人权。

41. 提供和接受情报，都能够对人权和基本自由产生重要影响。交付外国政府或情报部门的资料可能用于对个人权利的法律限制，也可能成为侵犯人权行为的根据。同样，从一外国实体收到的情报可能是以违反国际人权法的方式而获得。因此，在缔结一个共享协议或分享任何资料前，良好做法是情报部门对外国同行的人权和个人资料保护记录以及适用于这些部门的法律和制度保障(比如监督)进行一般性评估。[162] 在分享关于具体个人或群体的资料前，情报部门采取步骤评估可能对有关个人的影响。[163] 良好做法是，如果有合理的理由相信，共享资料可能导致对有关个人权利的侵犯，则绝对禁止共享任何资料。[164] 在某些情况下，如果共享情报助长严重侵犯人权行为的实施，则可能引发国家责任。另外，许多国家法律要求国家根据自身和对方任务评估共享某些资料的必要性。[165] 评估资料共享是否必要、是否与接受方的任务有关，使得情报部门能够恪守最低限度共享资料的原则；比如，情报部门尽最大可能把共享的个人资料数量降到最低程度。[166] 这是有助于防止过度或任意共享情报的保障。

42. 鉴于情报共享可能影响人权，良好做法是情报部门向外国实体交付前审查一切外传资料的准确性和相关性。[167] 如果怀疑外传情报的可靠性，则扣发或附以误差评估。[168] 最后，良好做法是以书面进行一切情报共享并予以记录；这有助于监督机构的后续审查。[169]

---

[162] Netherlands, Review Committee for the Security and Intelligence Services, review report on the cooperation of the GISS with Foreign intelligence and/or security services, pp. 7–11, 43; Arar Commission pp. 345, 348.

[163] Croatia (footnote 2), art. 60 (1); Germany (footnote 2), sect. 19; Switzerland (footnote 5), art. 17 (4); Netherlands, Review Committee for the Security and Intelligence Services, review report on the cooperation of the GISS with foreign intelligence and/or security services, p. 24.

[164] Canada, Arar Commission, p. 346–347.

[165] Croatia (footnote 2), art. 60 (1)(3); Germany (footnote 2), sect. 19, Germany (footnote 106), sect. 7 a (1)1; Switzerland (footnote 2), art. 17 (3).

[166] Canada, Arar Commission, pp. 338–339.

[167] Netherlands (footnote 20), arts. 41, 59; Canada, Arar Commission pp. 332, 334–336.

[168] Netherlands (footnote 20), art. 41. On this obligation in the context of domestic sharing, see South Africa (footnote 2), sect. 3(3).

[169] Netherlands (footnote 20), art. 42; Germany (footnote 2), sect. 19 (3)(4); Germany (footnote 106), sect. 7 a (3); Croatia (footnote 2), art. 60(3); Netherlands, Review Committee for the Security and Intelligence Services, review report on the cooperation of the GISS with foreign intelligence and/or security services, pp. 22–23.

做法 34. 独立监督机构能够审查情报共享协议和情报部门交付外国实体的任何资料。

43. 良好做法是：监督机构负责审查情报共享协议和在这些协议下所作的任何安排。[170] 独立监督机构能够审查情报共享协议的法律框架和程序事项，确保其符合国家法律和相关国际法律标准。作为一般性规则，监督机构有权获得一切对其执行任务有必要的资料(见做法 7)。然而，在国际情报共享方面，第三方规则可能要求限制监督机构接触外国实体提供的资料。一般认为监督机构属于第三方；因此它们通常不能接触外国实体与情报部门分享的资料。然而，监督机构有权审查向外国实体交付的资料，它们行使这一权力，属于审查情报部门所有方面活动的任务一部分(见做法 7)。在这方面，良好做法是国家法律明确要求情报部门向独立监督机构报告情报共享情况。[171] 这为情报共享做法的合法性提供一个核查措施，并且是防止共享可能对有关个人产生严重人权影响的个人资料的重要保障。

做法 35. 明确禁止情报部门以任何方式利用外国情报部门的协助，以规避国家法律标准和对自身活动的机构管理。如果国家请外国情报部门为其开展活动，则要求这些部门遵守本国情报部门开展活动时适用的同样法律标准。

44. 管辖情报部门活动的国家法律规定法律和机构保障，以在情报活动方面保护人权和宪法秩序。因此，如果各国或其情报部门请外国实体在其管辖范围内开展自身不能合法开展的活动，则有违法治。良好做法是，国家法律绝对禁止情报部门与外国实体合作以规避适用于自身活动的法律义务。[172] 另外，必须强调，各国负有国际法律义务，保障其管辖下所有个人的权利。这意味着它们有责任确保外国情报部门不在其领土上从事侵犯人权的活动，以及不参与任何这类活动。[173] 实际上，各国如果援助和协助另一国侵犯个人人权，则须承担国际责任。[174]

---

[170] Canada (footnote 6), art. 17(2); Canada, MacDonald Commission report, p. 1080; Canada, Arar Commission, p. 321; Venice Commission (2007), p. 182.

[171] Germany (footnote 106), sect. 7a (5–6); Croatia, Act on Personal Data Protection, art. 34.

[172] European Parliament Temporary Committee on the Echelon Interception System, report on the existence of a global system for the interception of private and commercial communications, A5-0264/2001, pp. 87–88 (hereafter European Parliament, Echelon report); Church Committee report, p. 306.

[173] Human Rights Committee, general comment No. 31 on the nature of the general legal obligation imposed on States parties to the Covenant (CCPR/C/21/Rev.1/Add.13), para. 10; European Parliament Echelon report, pp. 87–89.

[174] Human Rights Committee, general comment No. 31; General Assembly resolution 56/83, annex, art. 16; Secretary-General of the Council of Europe, Secretary-General's report under art. 52 of the European Convention on Human Rights on the question of secret detention and transport of detainees suspected of terrorist acts, notably by or at the instigation of foreign agencies, SG/Inf (2006) 5, paras. 23 and 101.

Annex

Good practices on legal and institutional frameworks for intelligence services and their oversight

Practice 1. Intelligence services play an important role in protecting national security and upholding the rule of law. Their main purpose is to collect, analyse and disseminate information that assists policymakers and other public entities in taking measures to protect national security. This includes the protection of the population and their human rights.

Practice 2. The mandates of intelligence services are narrowly and precisely defined in a publicly available law. Mandates are strictly limited to protecting legitimate national security interests as outlined in publicly available legislation or national security policies, and identify the threats to national security that intelligence services are tasked to address. If terrorism is included among these threats, it is defined in narrow and precise terms.

Practice 3. The powers and competences of intelligence services are clearly and exhaustively defined in national law. They are required to use these powers exclusively for the purposes for which they were given. In particular, any powers given to intelligence services for the purposes of counter-terrorism must be used exclusively for these purposes.

Practice 4. All intelligence services are constituted through, and operate under, publicly available laws that comply with the Constitution and international human rights law. Intelligence services can only undertake or be instructed to undertake activities that are prescribed by and in accordance with national law. The use of subsidiary regulations that are not publicly available is strictly limited, and such regulations are both authorized by and remain within the parameters of publicly available laws. Regulations that are not made public do not serve as the basis for any activities that restrict human rights.

Practice 5. Intelligence services are explicitly prohibited from undertaking any action that contravenes the Constitution or international human rights law. These prohibitions extend not only to the conduct of intelligence services on their national territory but also to their activities abroad.

Practice 6. Intelligence services are overseen by a combination of internal, executive, parliamentary, judicial and specialized oversight institutions whose mandates and powers are based on publicly available law. An effective system of intelligence oversight includes at least one civilian institution that is independent of both the intelligence services and the executive. The combined remit of oversight institutions covers all aspects of the work of intelligence services, including their compliance with the law； the effectiveness and efficiency of their activities； their finances； and their administrative practices.

Practice 7. Oversight institutions have the power, resources and expertise to initiate and conduct their own investigations, as well as full and unhindered access to the information, officials and installations necessary to fulfil their mandates. Oversight institutions receive the full cooperation of intelligence services and law enforcement authorities in hearing witnesses, as well as obtaining documentation and other evidence.

Practice 8. Oversight institutions take all necessary measures to protect classified information and personal data to which they have access during the course of their work. Penalties are provided for the breach of these requirements by members of oversight institutions.

Practice 9. Any individual who believes that her or his rights have been infringed by an intelligence service is able to bring a complaint to a court or oversight institution, such as an ombudsman, human rights commissioner or national human rights institution.

Individuals affected by the illegal actions of an intelligence service have recourse to an institution that can provide an effective remedy, including full reparation for the harm suffered.

Practice 10. The institutions responsible for addressing complaints and claims for effective remedy arising from the activities of intelligence services are independent of the intelligence services and the political executive. Such institutions have full and unhindered access to all relevant information, the necessary resources and expertise to conduct investigations, and the capacity to issue binding orders.

Practice 11. Intelligence services carry out their work in a manner that contributes to the promotion and protection of the human rights and fundamental freedoms of all individuals under the jurisdiction of the State. Intelligence services do not discriminate against individuals or groups on the grounds of their sex, race, colour, language, religion, political or other opinion, national or social origin, or other status.

Practice 12. National law prohibits intelligence services from engaging in any political activities or from acting to promote or protect the interests of any particular political, religious, linguistic, ethnic, social or economic group.

Practice 13. Intelligence services are prohibited from using their powers to target lawful political activity or other lawful manifestations of the rights to freedom of association, peaceful assembly and expression.

Practice 14. States are internationally responsible for the activities of their intelligence services and their agents, and any private contractors they engage, regardless of where these activities take place and who the victim of internationally wrongful conduct is. Therefore, the executive power takes measures to ensure and exercise overall control of and responsibility for their intelligence services.

Practice 15. Constitutional, statutory and international criminal law applies to members of intelligence services as much as it does to any other public official. Any exceptions allowing intelligence officials to take actions that would normally violate national law are strictly limited and clearly prescribed by law. These exceptions never allow the violation of peremptory norms of international law or of the human rights obligations of the State.

Practice 16. National laws provide for criminal, civil or other sanctions against any member, or individual acting on behalf of an intelligence service, who violates or orders an action that would violate national law or international human rights law. These laws also establish procedures to hold individuals to account for such violations.

Practice 17. Members of intelligence services are legally obliged to refuse superior orders that would violate national law or international human rights law. Appropriate protection is provided to members of intelligence services who refuse orders in such situations.

Practice 18. There are internal procedures in place for members of intelligence services to report wrongdoing. These are complemented by an independent body that has a mandate and access to the necessary information to fully investigate and take action to address wrongdoing when internal procedures have proved inadequate. Members of intelligence services who, acting in good faith, report wrongdoing are legally protected from any form of reprisal. These protections extend to disclosures made to the media or the public at large if they are made as a last resort and pertain to matters of significant public concern.

Practice 19. Intelligence services and their oversight institutions take steps to foster an institutional culture of professionalism based on respect for the rule of law and human rights. In particular, intelligence services are responsible for training their members on relevant provisions of national and international law, including international human rights law.

Practice 20： Any measures by intelligence services that restrict human rights and fundamental freedoms comply with the following criteria：

(a) They are prescribed by publicly available law that complies with international human rights standards；

(b) All such measures must be strictly necessary for an intelligence service to fulfil its legally prescribed mandate；

(c) Measures taken must be proportionate to the objective. This requires that intelligence services select the measure that least restricts human rights, and take special care to minimize the adverse impact of any measures on the rights of individuals, including, in particular, persons who are not suspected of any wrongdoing；

(d) No measure taken by intelligence services may violate peremptory norms of international law or the essence of any human right；

(e) There is a clear and comprehensive system for the authorization, monitoring and oversight of the use of any measure that restricts human rights；

(f) Individuals whose rights may have been restricted by intelligence services are able to address complaints to an independent institution and seek an effective remedy.

Practice 21. National law outlines the types of collection measures available to intelligence services； the permissible objectives of intelligence collection； the categories of persons and activities which may be subject to intelligence collection； the threshold of suspicion required to justify the use of collection measures； the limitations on the duration for which collection measures may be used； and the procedures for authorizing, overseeing and reviewing the use of intelligence-collection measures.

Practice 22. Intelligence-collection measures that impose significant limitations on human rights are authorized and overseen by at least one institution that is external to and independent of the intelligence services. This institution has the power to order the revision, suspension or termination of such collection measures. Intelligence collection measures that impose significant limitations on human rights are subject to a multilevel process of authorization that includes approval within intelligence services, by the political executive and by an institution that is independent of the intelligence services and the executive.

Practice 23. Publicly available law outlines the types of personal data that intelligence services may hold, and which criteria apply to the use, retention, deletion and disclosure of these data. Intelligence services are permitted to retain personal data that are strictly necessary for the purposes of fulfilling their mandate.

Practice 24. Intelligence services conduct regular assessments of the relevance and accuracy of the personal data that they hold. They are legally required to delete or update any information that is assessed to be inaccurate or no longer relevant to their mandate, the work of oversight institutions or possible legal proceedings.

Practice 25. An independent institution exists to oversee the use of personal data by intelligence services. This institution has access to all files held by the intelligence services and has the power to order the disclosure of information to individuals concerned, as well as the destruction of files or personal information contained therein.

Practice 26. Individuals have the possibility to request access to their personal data held by intelligence services. Individuals may exercise this right by addressing a request to a relevant authority or through an independent data-protection or oversight institution. Individuals have the right to rectify inaccuracies in their personal data. Any exceptions to these general rules are prescribed by law and strictly limited, proportionate and necessary

for the fulfilment of the mandate of the intelligence service. It is incumbent upon the intelligence service to justify, to an independent oversight institution, any decision not to release personal information.

Practice 27. Intelligence services are not permitted to use powers of arrest and detention if they do not have a mandate to perform law enforcement functions. They are not given powers of arrest and detention if this duplicates powers held by law enforcement agencies that are mandated to address the same activities.

Practice 28. If intelligence services have powers of arrest and detention, they are based on publicly available law. The exercise of these powers is restricted to cases in which there is reasonable suspicion that an individual has committed or is about to commit a specific criminal offence. Intelligence services are not permitted to deprive persons of their liberty simply for the purpose of intelligence collection. The use of any powers and arrest and detention by intelligence services is subject to the same degree of oversight as applies to their use by law enforcement authorities, including judicial review of the lawfulness of any deprivation of liberty.

Practice 29. If intelligence services possess powers of arrest and detention they comply with international human rights standards on the rights to liberty and fair trial, as well as the prohibition of torture and inhuman and degrading treatment. When exercising these powers, intelligence services comply with international standards set out in, inter alia, the Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment, the Code of Conduct for Law Enforcement Officials and the Basic Principles on the Use of Force and Firearms by Law Enforcement Officials.

Practice 30. Intelligence services are not permitted to operate their own detention facilities or to make use of any unacknowledged detention facilities operated by third parties.

Practice 31. Intelligence-sharing between intelligence agencies of the same State or with the authorities of a foreign State is based on national law that outlines clear parameters for intelligence exchange, including the conditions that must be met for information to be shared, the entities with which intelligence may be shared, and the safeguards that apply to exchanges of intelligence.

Practice 32. National law outlines the process for authorizing both the agreements upon which intelligence-sharing is based and the ad hoc sharing of intelligence. Executive approval is needed for any intelligence-sharing agreements with foreign entities, as well as for the sharing of intelligence that may have significant implications for human rights.

Practice 33. Before entering into an intelligence-sharing agreement or sharing intelligence on an ad hoc basis, intelligence services undertake an assessment of the counterpart's record on human rights and data protection, as well as the legal safeguards and institutional controls that govern the counterpart. Before handing over information, intelligence services make sure that any shared intelligence is relevant to the recipient's mandate, will be used in accordance with the conditions attached and will not be used for purposes that violate human rights.

Practice 34. Independent oversight institutions are able to examine intelligence-sharing arrangements and any information sent by intelligence services to foreign entities.

Practice 35. Intelligence services are explicitly prohibited from employing the assistance of foreign intelligence services in any way that results in the circumvention of national legal standards and institutional controls on their own activities. If States request foreign intelligence services to undertake activities on their behalf, they require these services to comply with the same legal standards that would apply if the activities were undertaken by their own intelligence services.